

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 9月21日

出 願 番 号

Application Number:

平成11年特許願第266853号

出 願 人

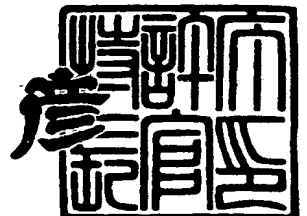
Applicant (s):

カシオ計算機株式会社

2000年 2月25日

特許庁長官  
Commissioner,  
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3009978

【書類名】 特許願

【整理番号】 99-0598-00

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/00  
G06F 13/00

【発明者】

【住所又は居所】 東京都羽村市栄町 3 丁目 2 番 1 号  
カシオ計算機株式会社羽村技術センター内

【氏名】 大塚 基

【特許出願人】

【識別番号】 000001443

【氏名又は名称】 カシオ計算機株式会社

【代理人】

【識別番号】 100074985

【弁理士】

【氏名又は名称】 杉村 次郎

【手数料の表示】

【予納台帳番号】 023180

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9109737

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 セキュリティ管理システムおよびそのプログラム記録媒体

【特許請求の範囲】

【請求項 1】

サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部供給するコンピュータシステムにおいて、前記サーバ装置は、接続された端末装置から固有の端末識別情報を読み込む読込手段と、

この読込手段によって読み込まれた固有の端末識別情報の他、アプリケーションソフト／データと共にその管理情報を記録媒体に書き込む書込手段と、

前記アプリケーションソフト／データの管理情報をスクランブル処理して暗号化するスクランブル処理手段とを具備し、

前記端末装置は、アプリケーションソフト／データが格納されている記録媒体がセットされている状態で、この記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から端末識別情報を読み出して自己の端末識別情報と比較する比較手段と、

この比較手段によって各端末識別情報の一致が検出された際に、前記スクランブル処理されているアプリケーションソフト／データの管理情報を復元するスクランブル復元手段とを具備したことを特徴とするセキュリティ管理システム。

【請求項 2】

前記サーバ装置は、前記読込手段によって端末装置から読み込んだ固有の端末識別情報を暗号化する暗号化手段を有し、前記書込手段は前記暗号化手段によって暗号化された端末識別情報を記録媒体に書き込み、

前記端末装置は、アプリケーションソフト／データおよび暗号化された端末識別情報が格納されている記録媒体がセットされている状態で、この記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から暗号化された端末識別情報を読み出してそれを復元する暗号復元手段を有し、前記比較手段は前記暗号復元手段によって復元された端末識別情報と自己の端末識別情報とを比較するようにしたことを特徴とする請求項 1 記載のセキュリティ管理シス

テム。

【請求項 3】

前記サーバ装置は、前記スクランブル処理手段によって前記アプリケーションソフト／データの管理情報をスクランブル処理した際に使用したスクランブル処理用の暗号キーを端末装置に書き込む書込手段を有し、

前記スクランブル復元手段は、前記スクランブル処理用の暗号キーを用いてアプリケーションソフト／データの管理情報を復元するようにしたことを特徴とする請求項 1 記載のセキュリティ管理システム。

【請求項 4】

サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して各端末装置側に外部供給するコンピュータシステムにおいて

前記サーバ装置は、接続された端末装置から固有の端末識別情報を読み込む読込手段と、

この読込手段によって読み込んだ固有の端末識別情報を暗号化する暗号化手段と、

この暗号化手段によって暗号化された固有の端末識別情報の他、アプリケーションソフト／データを記録媒体に書き込む書込手段とを具備し、

前記端末装置は、アプリケーションソフト／データおよび暗号化された端末識別情報が格納されている記録媒体が端末装置にセットされている状態で、この記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から暗号化された端末識別情報を読み出してそれを復元する暗号復元手段と、

この暗号復元手段によって復元された端末識別情報と自己の端末識別情報とを比較する比較手段と、

この比較手段によって各端末識別情報の一致が検出された際に、その記録媒体内のアプリケーションソフト／データに対するアクセスを許可するアクセス制御手段とを具備したことを特徴とするセキュリティ管理システム。

【請求項 5】

前記暗号化手段によって暗号化された固有の端末識別情報と共に、アプリケー

ションソフトを記録媒体に書き込む際に、前記書込手段はアプリケーションソフトに対応付けてそのアクセス制御用のプログラムとこのアクセス制御用プログラム内に前記暗号化された固有の端末識別情報を組み込み、

前記端末装置は、アプリケーションソフト内に前記アクセス制御用プログラムおよび端末識別情報が組み込まれている記録媒体がセットされた場合に、この記録媒体内のアクセス制御用プログラムを起動させると共に、このアクセス制御用プログラムにしたがって前記暗号化端末識別情報を読み出してそれを復元すると共に、復元された端末識別情報と当該端末装置から読み出した端末識別情報とを比較し、この結果、各端末識別情報の一致が検出された場合には、記録媒体内の対応するアプリケーションソフトのアクセスを許可し、各端末識別情報の不一致が検出された場合には、そのアプリケーションソフトのアクセスを禁止するようにしたことを特徴とする請求項 4 記載のセキュリティ管理システム。

#### 【請求項 6】

前記サーバ装置は、同一グループに属する複数台の端末装置を識別するグループ識別情報と前記読込手段によって読み込んだ固有の端末識別情報とに基づいてそのグループ固有のグループ端末識別情報を生成する生成手段を有し、

前記書込手段は前記生成手段によって生成されたグループ端末識別情報を記録媒体と端末装置にそれぞれ書き込み、

前記端末装置は、アプリケーションソフト／データおよびグループ端末識別情報が格納されている記録媒体がセットされている状態で、この記録媒体内のアプリケーションソフト／データをアクセスする際に、前記比較手段は、サーバ装置から当該端末装置に書き込まれたグループ端末識別情報と当該記録媒体から読み出されたグループ端末識別情報とを比較するようにしたことを特徴とする請求項 1 あるいは 4 記載のセキュリティ管理システム。

#### 【請求項 7】

前記サーバ装置は、前記暗号化手段によって端末識別情報を暗号化した際に使用した端末識別情報用の暗号キーを端末装置に書き込む書込手段を有し、

前記端末装置は、アプリケーションソフト／データおよび暗号化された端末識別情報が格納されている記録媒体がセットされている状態で、この記録媒体内の

アプリケーションソフト／データをアクセスする際に、前記暗号復元手段は前記端末識別情報用の暗号キーを用いて当該記録媒体内の暗号化端末識別情報を復元するようにしたことを特徴とする請求項 2 あるいは 4 記載のセキュリティ管理システム。

【請求項 8】

コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、  
接続された端末装置から固有の端末識別情報を読み込ませるコンピュータが読み取り可能なプログラムコードと、

読み込まれた固有の端末識別情報の他、アプリケーションソフト／データと共にその管理情報を記録媒体に書き込ませるコンピュータが読み取り可能なプログラムコードと、

前記アプリケーションソフト／データの管理情報をスクランブル処理させるコンピュータが読み取り可能なプログラムコードと、

アプリケーションソフト／データが格納されている記録媒体が端末装置にセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から端末識別情報を読み出して自己の端末識別情報と比較させるコンピュータが読み取り可能なプログラムコードと、

この結果、各端末識別情報の一致が検出された際に、前記スクランブル処理されているアプリケーションソフト／データの管理情報を復元させるコンピュータが読み取り可能なプログラムコードとを有する記録媒体。

【請求項 9】

コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、

接続された端末装置から固有の端末識別情報を読み込ませるコンピュータが読み取り可能なプログラムコードと、

端末装置から読み込んだ固有の端末識別情報を暗号化させるコンピュータが読み取り可能なプログラムコードと、

暗号化された固有の端末識別情報の他、アプリケーションソフト／データを記録媒体に書き込ませるコンピュータが読み取り可能なプログラムコードと、

アプリケーションソフト／データおよび暗号化された端末識別情報が格納され

ている記録媒体が端末装置にセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から暗号化された端末識別情報を読み出してそれを復元させるコンピュータが読み取り可能なプログラムコードと、

復元された端末識別情報と自己の端末識別情報とを比較させるコンピュータが読み取り可能なプログラムコードと、

各端末識別情報の一致が検出された際に、その記録媒体内のアプリケーションソフト／データに対するアクセスを許可させるコンピュータが読み取り可能なプログラムコードとを有する記録媒体。

【請求項 1 0】

コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、

接続された端末装置から固有の端末識別情報を読み込ませるコンピュータが読み取り可能なプログラムコードと、

読み込まれた固有の端末識別情報の他、アプリケーションソフト／データと共にその管理情報を記録媒体に書き込ませるコンピュータが読み取り可能なプログラムコードと、

前記記録媒体に書き込まれたアプリケーションソフト／データの管理情報をスクランブル処理させるコンピュータが読み取り可能なプログラムコードとを有する記録媒体。

【請求項 1 1】

コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、

アプリケーションソフト／データが格納されている記録媒体が端末装置にセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から端末識別情報を読み出して自己の端末識別情報と比較させるコンピュータが読み取り可能なプログラムコードと、

この結果、各端末識別情報の一致が検出された際に、前記スクランブル処理されているアプリケーションソフト／データの管理情報を復元させるコンピュータが読み取り可能なプログラムコードとを有する記録媒体。

【請求項 1 2】

コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、  
接続された端末装置から固有の端末識別情報を読み込ませるコンピュータが読み取り可能なプログラムコードと、  
端末装置から読み込んだ固有の端末識別情報を暗号化させるコンピュータが読み取り可能なプログラムコードと、  
暗号化された固有の端末識別情報の他、アプリケーションソフト／データを記録媒体に書き込ませるコンピュータが読み取り可能なプログラムコードとを有する記録媒体。

【請求項 1 3】

コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、  
アプリケーションソフト／データおよび暗号化された端末識別情報が格納されている記録媒体が端末装置にセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から暗号化された端末識別情報を読み出してそれを復元させるコンピュータが読み取り可能なプログラムコードと、

復元された端末識別情報と自己の端末識別情報とを比較させるコンピュータが読み取り可能なプログラムコードと、

各端末識別情報の一致が検出された際に、その記録媒体内のアプリケーションソフト／データに対するアクセスを許可させるコンピュータが読み取り可能なプログラムコードとを有する記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

この発明は、サーバ側のアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末側に外部供給するコンピュータシステムにおいて、記録媒体内のアプリケーションソフト／データに対する安全性を保障するセキュリティ管理システムおよびそのプログラム記録媒体に関する。

【0 0 0 2】

【従来の技術】



一般に、アプリケーションソフトはフロッピーディスクやコンパクトディスク等の記録媒体を介してパーソナルコンピュータに別途提供され、これをインストールすることにより起動される。この場合、ソフトメーカはアプリケーションソフトにユニークなプロダクト番号を付けて出荷する。このソフトをユーザがパソコン上でインストールして動作させる場合、許可キーとしてこのプロダクト番号をキーボードから入力するようにしている。

一方、複数台の端末装置がネットワークを介して通信接続されてなるオンライン型のクライアント・サーバシステムにおいて、各クライアント端末はネットワークを介してアプリケーションソフトを入手するようにしている。

【 0 0 0 3 】

【発明が解決しようとする課題】

しかしながら、記録媒体を介して提供されるアプリケーションソフトは、そのプロダクト番号さえ分かれば、複数台のパソコンに何回でもインストールすることができ、不法なコピー複製が可能となる。このようなコピー複製を禁止するためには、一旦、アプリケーションソフトをインストールしたらその記録媒体の内容を全てクリアする必要がある。しかしながら、記録媒体内の内容を全てクリアしてしまうと、その後、障害が発生し、再度インストールする必要が生じた時には、それに対応することができなくなり、まは、記録媒体の内容をその都度クリアするという面倒な作業を強要することにもなる。

また、ネットワーク経由でクライアント端末からサーバーへアクセスする場合、ユーザIDとパスワードとを知っていれば、誰でもどの端末からでもアプリケーションソフトをアクセスすることができ、不正なアクセスの可能性がある。

ことことはアプリケーションソフトに限らず、企業情報などの機密性の高い重要データが格納されている記録媒体を介して端末装置に提供する場合であっても同様であり、この記録媒体を誤って紛失してしまうと第三者に重要データを見られてしまい、セキュリティ維持の点で問題があった。

第1の発明の課題は、サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部提供する場合、記録媒体と端末装置との対応付けを端末識別情報の一致、不一致およびアプリケーション

ョンソフト／データを管理する管理情報の暗号化、複合化によって行うことで、特定の端末装置に対してのみアプリケーションソフト／データのアクセスを許可できるようにすることである。

第 2 の発明の課題は、サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部提供する場合、記録媒体と端末装置との対応付けを端末識別情報の暗号化、複合化によって行うことで、特定の端末装置に対してのみアプリケーションソフト／データのアクセスを許可できるようにすることである。

【 0 0 0 4 】

この発明の手段は、次の通りである。

請求項第 1 記載の発明（第 1 の発明）は、サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部供給するコンピュータシステムにおいて、前記サーバ装置は、接続された端末装置から固有の端末識別情報を読み込む読込手段と、この読込手段によって読み込まれた固有の端末識別情報の他、アプリケーションソフト／データと共にその管理情報を記録媒体に書き込む書込手段と、前記アプリケーションソフト／データの管理情報をスクランブル処理して暗号化するスクランブル処理手段とを具備し、前記端末装置は、アプリケーションソフト／データが格納されている記録媒体がセットされている状態で、この記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から端末識別情報を読み出して自己の端末識別情報と比較する比較手段と、この比較手段によって各端末識別情報の一致が検出された際に、前記スクランブル処理されているアプリケーションソフト／データの管理情報を復元するスクランブル復元手段とを具備するものである。

なお、この発明は次のようなものであってもよい。

(1) 前記サーバ装置は、前記読込手段によって端末装置から読み込んだ固有の端末識別情報を暗号化する暗号化手段を有し、前記書込手段は前記暗号化手段によって暗号化された端末識別情報を記録媒体に書き込み、前記端末装置は、アプリケーションソフト／データおよび暗号化された端末識別情報が格納されている記録媒体がセットされている状態でこの記録媒体内のアプリケーションソフト

／データをアクセスする際に、当該記録媒体から暗号化された端末識別情報を読み出してそれを復元する暗号復元手段を有し、前記比較手段は前記暗号復元手段によって復元された端末識別情報と自己の端末識別情報とを比較する。

この場合、前記サーバ装置は、前記暗号化手段によって端末識別情報を暗号化した際に使用した端末識別情報用の暗号キーを端末装置に書き込む書込手段を有し、前記端末装置は、アプリケーションソフト／データおよび暗号化された端末識別情報が格納されている記録媒体がセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、前記暗号復元手段は前記端末識別情報用の暗号キーを用いて当該記録媒体内の暗号化端末識別情報を復元する。

(2) 前記サーバ装置は、前記スクランブル処理手段によって前記アプリケーションソフト／データの管理情報をスクランブル処理した際に使用したスクランブル処理用の暗号キーを端末装置に書き込む書込手段を有し、前記スクランブル復元手段は、前記スクランブル処理用の暗号キーを用いてアプリケーションソフト／データの管理情報を復元する。

(3) 前記サーバ装置は、同一グループに属する複数台の端末装置を識別するグループ識別情報と前記読込手段によって読み込んだ固有の端末識別情報とに基づいてそのグループ固有のグループ端末識別情報を生成する生成手段を有し、前記書込手段は前記生成手段によって生成されたグループ端末識別情報を記録媒体と端末装置にそれぞれ書き込み、前記端末装置は、アプリケーションソフト／データおよびグループ端末識別情報が格納されている記録媒体がセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、前記比較手段は、サーバ装置から当該端末装置に書き込まれたグループ端末識別情報と当該記録媒体から読み出されたグループ端末識別情報とを比較する。

請求項 1 記載の発明においては、サーバ装置は、接続された端末装置から固有の端末識別情報を読み込むと共に、読み込んだ固有の端末識別情報の他、アプリケーションソフト／データとその管理情報を記録媒体に書き込む。そして、前記アプリケーションソフト／データの管理情報をスクランブル処理して暗号化する。前記端末装置は、アプリケーションソフト／データが格納されている記録媒体

がセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から端末識別情報を読み出して自己の端末識別情報と比較し、その結果、各端末識別情報の一致が検出された際に、前記スクランブル処理されているアプリケーションソフト／データの管理情報を復元する

したがって、サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部提供する場合、記録媒体と端末装置との対応付けを端末識別情報の一致、不一致およびアプリケーションソフト／データを管理する管理情報の暗号化、複合化によって行うことで、特定の端末装置に対してのみアプリケーションソフト／データのアクセスを許可することができる。

【 0 0 0 5 】

請求項第 2 記載の発明（第 2 の発明）は、サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して各端末装置側に外部供給するコンピュータシステムにおいて、前記サーバ装置は、接続された端末装置から固有の端末識別情報を読み込む読込手段と、この読込手段によって読み込んだ固有の端末識別情報を暗号化する暗号化手段と、この暗号化手段によって暗号化された固有の端末識別情報の他、アプリケーションソフト／データを記録媒体に書き込む書込手段とを具備し、前記端末装置は、アプリケーションソフト／データおよび暗号化された端末識別情報が格納されている記録媒体が端末装置にセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から暗号化された端末識別情報を読み出してそれを復元する暗号復元手段と、この暗号復元手段によって復元された端末識別情報と自己の端末識別情報とを比較する比較手段と、この比較手段によって各端末識別情報の一致が検出された際に、その記録媒体内のアプリケーションソフト／データに対するアクセスを許可するアクセス制御手段とを具備するものである。

なお、この発明は次のようなものであってもよい。

（１）前記暗号化手段によって暗号化された固有の端末識別情報と共に、アプリケーションソフトを記録媒体に書き込む際に、前記書込手段はアプリケーションソフトに対応付けてそのアクセス制御用のプログラムとこのアクセス制御用プ

プログラム内に前記暗号化された固有の端末識別情報を組み込み、前記端末装置は、アプリケーションソフト内に前記アクセス制御用プログラムおよび端末識別情報が組み込まれている記録媒体がセットされた場合、この記録媒体内のアクセス制御用プログラムを起動させると共に、このアクセス制御用プログラムにしたがって前記暗号化端末識別情報を読み出してそれを復元すると共に、復元された端末識別情報と当該端末装置から読み出した端末識別情報とを比較し、この結果、各端末識別情報の一致が検出された場合には、記録媒体内の対応するアプリケーションソフトのアクセスを許可し、各端末識別情報の不一致が検出された場合には、そのアプリケーションソフトのアクセスを禁止する。

(2) 前記サーバ装置は、同一グループに属する複数台の端末装置を識別するグループ識別情報と前記読込手段によって読み込んだ固有の端末識別情報とに基づいてそのグループ固有のグループ端末識別情報を生成する生成手段を有し、前記書込手段は前記生成手段によって生成されたグループ端末識別情報を記録媒体に書き込み、前記端末装置は、アプリケーションソフト／データおよびグループ端末識別情報が格納されている記録媒体がセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、前記比較手段は、サーバ装置から当該端末装置に書き込まれたグループ端末識別情報と当該記録媒体から読み出されたグループ端末識別情報とを比較する。

(3) 前記サーバ装置は、前記暗号化手段によって端末識別情報を暗号化した際に使用した端末識別情報用の暗号キーを端末装置に書き込む書込手段を有し、

前記端末装置は、アプリケーションソフト／データおよび暗号化された端末識別情報が格納されている記録媒体がセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、前記暗号復元手段は前記端末識別情報用の暗号キーを用いて当該記録媒体内の暗号化端末識別情報を復元する。

請求項 2 記載の発明においては、サーバ装置は、接続された端末装置から固有の端末識別情報を読み込むと共に、それを暗号化する。そして、暗号化した固有の端末識別情報の他、アプリケーションソフト／データを記録媒体に書き込む。端末装置は、アプリケーションソフト／データおよび暗号化された端末識別情報

が格納されている記録媒体が端末装置にセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から暗号化された端末識別情報を読み出してそれを復元すると共に、復元された端末識別情報と自己の端末識別情報とを比較し、この結果、各端末識別情報の一致が検出された際に、その記録媒体内のアプリケーションソフト／データに対するアクセスを許可する。

したがって、サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部提供する場合、記録媒体と端末装置との対応付けを端末識別情報の暗号化、複合化によって行うことで、特定の端末装置に対してのみアプリケーションソフト／データのアクセスを許可することができる。

【0006】

#### 【発明の実施の形態】

##### （第1実施形態）

以下、図1～図7を参照してこの発明の第1実施形態を説明する。

図1は、この実施形態におけるセキュリティ管理システムの全体構成を示したブロック図である。

このセキュリティ管理システムは、サーバ装置側で記憶管理されているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部提供するもので、この記録媒体内のアプリケーションソフト／データに対してセキュリティ維持を図り、第三者による複製コピー等を防止するようにしている。すなわち、このシステムは、例えば、会社組織において会社側に設置させているサーバ装置1と、各営業担当者が持参するモバイル型のクライアント端末（携帯端末装置）2とを有し、各営業担当者は外出先で可搬型記録媒体3内のアプリケーションソフト／データをアクセスしながら営業活動を行い、そして、1日の営業終了時に端末本体から可搬型記録媒体3を抜き取り、それをサーバ装置1側のカードライター4にセットすると、サーバ装置1はカードライター4を介して記録媒体3内の営業記録を収集処理するようにしている。そして、サーバ装置1と複数台の携帯端末装置2とはシリアルケーブル5を介して着脱自在に接続可能となっ

ている。すなわち、サーバ装置 1 と複数台の携帯端末装置 2 とは必要に応じて接続することができるようになっている。

#### 【0007】

可搬型記録媒体 3 は例えば、コンパクトフラッシュカードによって構成されているもので、以下、コンパクトフラッシュカードを CF カードと称する。ここで、図中、各 CF カードに付した「# A」「# B」「# C」、……は、端末名称「A」「B」「C」、……で示される携帯端末装置 2 に対応付けられた端末対応のカードであることを示している。なお、この実施形態においては端末対応のカードの他、後述する端末グループ対応のカードも存在するが、図 1 の例では端末対応のカードのみを示している。カードライタ 4 は CF カード 3 を複数枚同時にセット可能なもので、複数のカード挿入口を有している。

そして、サーバ装置 1 は CF カード 3 を介して携帯端末装置 2 側にアプリケーションソフト／データベースファイル（以下 AP ソフト／データと称する）を配布する。すなわち、サーバ装置 1 は CF カード 3 に書き込む書込対象、つまり、配布対象の AP ソフト／データが任意に指定された際に、AP ソフト／データベース格納部 6 をアクセスしてそれに対応する AP ソフト／データを呼び出してカードライタ 4 に与え、それにセットされている 1 または 2 以上の CF カード 3 に AP ソフト／データを書き込む。

#### 【0008】

その際、CF カード 3 に格納した AP ソフト／データの管理情報、つまり、FAT (File Allocation Table) およびループディレクトリの領域を指定してその内容をスクランブル処理（暗号化処理）するが、この場合、スクランブル処理用として任意に生成された暗号キーを用いてスクランブルが行われる。なお、スクランブル処理（暗号化処理）をどのような手法で行うかは、任意であり、任意に生成された暗号キーを用いて AP ソフト／データの管理情報を暗号化するようにしている。また、各携帯端末装置 2 には予め設定されている固有の端末識別情報（製造番号）が記憶されており、サーバ装置 1 は各携帯端末装置 2 から固有の端末識別情報（製造番号）を読み込むと、任意に生成された暗号キーを用いて端末識別情報を暗号化し、CF カード 3 に書き込む。そして

、この端末識別情報の暗号化に使用された暗号キーとスクランブル処理時に使用された暗号キーは、携帯端末装置 2 に書き込まれる。

【0009】

携帯端末装置 2 は、A P ソフト／データが格納されている C F カード 3 がカードライタ 7 にセットされている状態で、この C F カード 3 内の A P ソフト／データをアクセスする際に、このカードから暗号化端末識別情報を読み出すと共に、サーバ装置 1 から自己のメモリに書き込まれている端末識別情報用の暗号キーを読み出し、この暗号キーを用いて暗号化端末識別情報を復元する。そして、自己メモリに予め設定されている端末識別情報を呼び出し、復元した端末識別情報と自己の設定端末識別情報とを比較する。この結果、各端末識別情報の一致が検出された際に、スクランブル処理されている A P ソフト／データの管理情報を復元する。その際、スクランブル処理用の暗号キーを読み出して A P ソフト／データの F A T およびルートディレクトリを復元することにより、A P ソフト／データに対するアクセスを許可するようにしている。

【0010】

図 2 は、C F カード 3 の内容を示した図で、サーバ装置 1 によって C F カード 3 には「スクランブルフラグ」、「暗号化識別情報」、「F A T」、「ルートディレクトリ」、「A P ソフト／データ」が書き込まれる。ここで、「スクランブルフラグ」は、C F カード 3 内に格納されている A P ソフト／データの「F A T」、「ルートディレクトリ」がスクランブル処理されている状態にあることを示すフラグであり、また「暗号化識別情報」は携帯端末装置 2 から読み込んだ固有の端末識別情報（製造番号）がサーバ装置 1 によって暗号化されたものである。「F A T」、「ルートディレクトリ」は配布対象としての 1 または 2 以上の A P ソフト／データを管理する管理情報であり、その内容はスクランブル処理されている。

【0011】

図 3 は、例えば、グループ「営業 1 課」、「営業 2 課」……のように端末グループ対応の C F カード 3 を示した図で、図中、「# A 1」、「# A 2」、「# A 3」で示す各 C F カード 3 は、端末名称が「A 1」、「A 2」、「A 3」である各



携帯端末装置 2 が属する端末グループ A 対応の記録媒体であり、同様に、「# B 1」、「# B 2」……で示す各 C F カード 3 は、端末名称が「B 1」、「B 2」、……である各携帯端末装置 2 が属する端末グループ B 対応の記録媒体であり、同一グループ内の各 C F カード 3 はそのグループに属する各携帯端末装置 2 で共通して使用することができるようになっている。この端末グループ対応の C F カード 3 内にはグループ端末識別情報が書き込まれる。このグループ端末識別情報はそのグループに属する 1 台目の携帯端末装置 2 から読み込んだ固有の端末識別情報（製造番号）と、任意に入力したグループ名との組み合わせによって生成されたもので、同一グループの各 C F カード 3 には、同一のグループ端末識別情報が書き込まれる。

#### 【 0 0 1 2 】

図 4 は、サーバ装置 1 / 各端末装置 2 の全体構成を示したブロック図であり、それらは基本的に同様の構成となっているため、同一符号を付して示す。

C P U 1 1 は、記憶装置 1 2 内のオペレーティングシステムや各種アプリケーションソフトにしたがってこのサーバ装置 1 や端末装置 2 の全体動作を制御する中央演算処理装置である。記憶装置 1 2 は、オペレーティングシステムや各種アプリケーションソフトの他、データベース、文字フォント等が格納され、磁氣的、光学的、半導体メモリ等によって構成されている記録媒体 1 3 やその駆動系を有している。この記録媒体 1 3 はハードディスク等の固定的な媒体若しくは着脱自在に装着可能な C D - R O M、フロッピーデスク、R A M カード、磁気カード等の可搬型の媒体である。また、この記録媒体 1 3 内のプログラムやデータは、必要に応じて C P U 1 1 の制御により R A M（例えば、スタティック R A M）1 4 にロードされたり、R A M 1 4 内のデータが記録媒体 1 3 にセーブされる。更に、記録媒体はサーバ等の外部機器側に設けられているものであってもよく、C P U 1 1 は伝送媒体を介してこの記録媒体内のプログラム／データを直接アクセスして使用することもできる。

また、C P U 1 1 は記録媒体 3 内に格納されるその一部あるいは全部を他の機器側から伝送媒体を介して取り込み、記録媒体 1 3 に新規登録あるいは追加登録することもできる。すなわち、コンピュータ通信システムを構成する他の機器（

例えば、サーバ・ホスト・クライアントコンピュータ) から通信回線やケーブル等の有線伝送路あるいは電波、マイクロウェーブ、赤外線等の無線伝送路を介して送信されてきたプログラム／データを伝送制御部 15 によって受信して記録媒体 13 内にインストールすることができる。更に、プログラム／データはサーバ等の外部機器側で記憶管理されているものであってもよく、CPU 11 は伝送媒体を介して外部機器側のプログラム／データを直接アクセスして使用することもできる。

#### 【0013】

このように CPU 11 は、予め固定的に常駐されているプログラム／データに限らず、記録媒体や伝送媒体を介して外部供給されたプログラム／データを利用して、あるいは外部機器側で記憶管理されているプログラム／データを直接利用してこの実施形態特有の動作を実行することもできる。一方、CPU 11 にはその入出力周辺デバイスである伝送制御部 15、入力部 16、表示部 17、印字部 18、カードリーダー／ライター 19 がバスラインを介して接続されており、入出力プログラムにしたがって CPU 11 はそれらの動作を制御する。伝送制御部 15 は、例えば、通信モデムや赤外線モジュールあるいはアンテナ等を含む通信インターフェイスである。入力部 16 はキーボードやタッチパネルあるいはマウスやタッチ入力ペン等のポインティングデバイスを構成する操作部であり、文字列データや各種コマンドを入力する。なお、表示部 17 は、フルカラー表示を行う液晶や CRT あるいはプラズマ表示装置などであり、印字部 18 は熱転写やインクジェットなどのノンインパクトプリンタあるいはドットインパクトプリンタである。カードリーダー／ライター 19 は CF カード 3 に対してその書き込み／読み込み動作を行う。

#### 【0014】

次に、この第 1 実施形態におけるサーバ装置 1、携帯端末装置 2 の動作を図 5 ～図 7 に示すフローチャートを参照して説明する。ここで、これらのフローチャートに記述されている各機能を実現するためのプログラムは、読み取り可能なプログラムコードの形態で記録媒体 13 に格納されており、CPU 11 はこのプログラムコードにしたがった動作を逐次実行する。また、CPU 11 は伝送媒体を

介して伝送されてきた上述のプログラムコードにしたがった動作を逐次実行することもできる。このことは、後述する他の実施形態においても同様であり、記録媒体の他、伝送媒体を介して外部供給されたプログラム／データを利用してこの実施形態特有の動作を実行することもできる。

#### 【0015】

図5および図6は、サーバ装置1に携帯端末装置2、CFカード3が接続されている状態で、サーバ装置1側で記憶管理されているAPソフト／データを持ち運び自在なCFカード3を介して端末装置2側に外部提供する場合におけるサーバ装置1側の動作を示したフローチャートである。

まず、ユーザは書き込み対象のAPソフト／データを全て選択すると（ステップA1）、CPU11はAPソフト／データベース格納部6から選択指定されたAPソフト／データおよびそのFAT、ルートディレクトリを取得しておく（ステップA2）。また、ユーザは書き込み対象の端末を指定すると（ステップA3）、その指定内容に応じて指定端末のみの書き込みか、グループ対応書き込みかを調べる（ステップA4）。いま、指定端末のみの書き込みが指定された場合には、指定端末から「製造番号」を読み出すと共に（ステップA5）、それを暗号化するための暗号キーを生成する（ステップA6）。この場合、暗号キーはランダムに生成した数値データ等であり、指定端末から読み出した「製造番号」をこの暗号キーを用いて暗号化し、端末識別情報を生成する（ステップA7）。

#### 【0016】

そして、スクランブル処理用の暗号キーを生成するが（ステップA8）、この暗号キーもランダムに生成した数値データ等である。このようにして生成した端末識別情報暗号用の暗号キーと、スクランブル処理用の暗号キーとを指定端末に書き込む（ステップA9）。また、指定端末対応のCFカード3には、ステップA2で取得したAPソフト／データとそのFAT、ルートディレクトリおよびステップA7で暗号化した端末識別情報を書き込む（ステップA10）。そして、CFカード3に書き込んだAPソフト／データのFATとルートディレクトリをステップA8で生成した暗号キーを用いてスクランブル処理して暗号化すると共に（ステップA11）、そのCFカード3内の「スクランブルフラグ」をONす

る（ステップ A 1 2）。これによって指定端末に対する処理が終わると、ステップ A 1 3 でそのことが検出されてこのフローの終了となる。

【0 0 1 7】

一方、グループ対応の書き込みが指定された場合には（ステップ A 4）、図6のフローチャートに進み、先ず、そのグループ端末識別情報を生成する処理が行われる。すなわち、上述したようにグループ端末識別情報は、そのグループに属する 1 台目の携帯端末装置 2 から読み込んだ固有の端末識別情報（製造番号）と、任意に入力したグループ名との組み合わせによって生成するようにしているため、グループ内の 1 台目の端末であれば（ステップ A 1 5）、そのグループ識別情報（グループ名）を任意に入力すると（ステップ A 1 6）、その 1 台目の端末から端末識別情報（製造番号）を読み出し（ステップ A 1 7）、このグループ名と製造番号とに基づいてそのグループ固有のグループ端末識別情報を生成する（ステップ A 1 8）。例えば、グループ名が「営業 1 課」、製造番号が「C 0 0 0 1」であれば、グループ端末識別情報として「C 0 0 0 1 営業 1 課」が生成される。

そして、このグループ端末識別情報を暗号化するための暗号キーをランダム生成すると共に（ステップ A 1 9）、この生成キーを用いてグループ端末識別情報を暗号化する（ステップ A 2 0）。また、スクランブル処理用の暗号キーを生成しておく（ステップ A 2 1）。次に、グループ端末識別情報と共に、その暗号化キーおよびスクランブル処理用の暗号キーを指定端末、この場合、1 台目の携帯端末装置 2 に書き込む（ステップ A 2 2）。

【0 0 1 8】

そして、図 5 のステップ A 1 0 に戻り、指定端末対応の C F カード 3 に、A P ソフト／データとその F A T、ルートディレクトリ、暗号化グループ端末識別情報を書き込む。そして、その F A T、ルートディレクトリをスクランブル処理用の暗号キーを用いてスクランブル処理すると共に（ステップ A 1 1）、スクランブルフラグを O N させる（ステップ A 1 2）。このような処理は指定グループ内の全端末に対して実行される。すなわち、ステップ A 1 3 では指定グループ内の全端末終了かを調べ、終了していなければ、ステップ A 1 4 に進み、同一グルー

プ内の次の端末を指定したのち、図 6 のステップ A 1 5 に進み、グループ端末識別情報と共に、その暗号化キーおよびスクランブル処理用の暗号キーを指定端末、この場合、2 台目の携帯端末装置 2 に書き込む。以下、指定グループ内の全端末終了まで上述の動作を繰り返すことにより、同一グループの各携帯端末装置 2 には同一の内容が書き込まれると共に、そのグループの書く携帯端末装置 2 および CF カード 3 には、同一のグループ端末識別情報が書き込まれる。

## 【0 0 1 9】

図 7 は、各携帯端末装置 2 側での動作を示したフローチャートであり、CF カード 3 へのアクセスが指定された際に、このフローチャートにしたがった動作が実行開始される。

まず、CPU 1 1 は CF カード 3 がセットされているかを調べ（ステップ B 1）、セットされていなければ、通常処理のメインフローに戻るが、セットされていれば、その CF カード 3 から端末識別情報を読み出すと共に（ステップ B 2）、サーバ装置 1 から自己の端末に書き込まれた端末情報暗号用の暗号キーを読み出し（ステップ B 3）、この端末識別情報を暗号キーに基づいて複合化する（ステップ B 4）。そして、予め自己の設定情報である端末識別情報を読み出し（ステップ B 5）、複合化した端末識別情報と比較し（ステップ B 6）、両者が一致するかを調べる（ステップ B 7）。

## 【0 0 2 0】

ここで、不一致が検出された場合には、当該カードに対するアクセスを不可として処理終了となるが、両者の一致が検出された場合には、CF カード 3 内のスクランブルフラグは ON されているかを調べる（ステップ B 8）。ここで、スクランブルフラグが ON されていなければ、端末識別情報の一致のみを条件として CF カード 3 に対するアクセスを許可するが、スクランブルフラグが ON されていれば、サーバ装置 1 から自己の端末に書き込まれたスクランブル処理用の暗号キーを読み出し（ステップ B 9）、CF カード 3 内の FAT、ルートディレクトリをこの暗号キーに基づいて複合化する（ステップ B 1 0）。これによって CF カード 3 へのアクセスが可能となる。

## 【0 0 2 1】

以上のように、この第 1 実施形態において、サーバ装置 1 は、接続された携帯端末装置 2 から固有の端末識別情報を読み込むと共に、読み込んだ固有の端末識別情報の他、A P ソフト／データとその F A T、ルートディレクトリを C F カード 3 に書き込み、更に、C F カード 3 内の F A T、ルートディレクトリをスクランブル処理して暗号化する。一方、携帯端末装置 2 は、A P ソフト／データが格納されている C F カード 3 がセットされている状態において、この C F カード 3 内の A P ソフト／データをアクセスする際に、当該 C F カード 3 から暗号化された端末識別情報を読み出してそれを復元し、自己の端末識別情報と比較した結果、それらの一致が検出された際に、スクランブル処理されている A P ソフト／データの F A T、ルートディレクトリを復元するようにしたから、その C F カード 3 に対するアクセスを許可することができる。すなわち、サーバ装置 1 側で管理している A P ソフト／データを持ち運び自在な C F カード 3 を介して携帯端末装置 2 側に外部提供する場合、C F カード 3 と携帯端末装置 2 との対応付けを端末識別情報の一致、不一致および A P ソフト／データの F A T、ルートディレクトリの暗号化、複合化によって行うことで、特定の端末に対してのみ A P ソフト／データのアクセスを許可することができ、端末毎のアクセス制御によってアクセス権限を有しない他の端末による不法なコピー複製を効果的に禁止することができるようになる。この場合、端末識別情報および A P ソフト／データの F A T、ルートディレクトリを暗号化するようにしたから、安全性はきわめて高くなる。

このことは、端末対応のカードに限らず、グループ対応のカードについても同様であり、例えば、営業地域毎に特定の A P ソフト／データを使用する場合、地域毎に端末グループを分けておけば、地域毎のアクセス制御が可能となる。

#### 【 0 0 2 2 】

##### (第 2 実施形態)

以下、この発明の第 2 実施形態について図 8 ～ 図 1 0 を参照して説明する。なお、上述した第 1 実施形態は、C F カード 3 毎のアクセス制御を示したが、この第 2 実施形態は C F カード 3 内に書き込まれている A P ソフト毎にアクセス制御を行うようにしたものである。そして、A P ソフトの F A T、ルートディレクトリに対するスクランブル処理は行わず、また、A P ソフト内にそのアクセスを制

御する制御プログラムと暗号化された端末識別情報を組み込むようにしている。ここで、両実施形態において基本的に同一のものは、同一符号を付して示し、その説明を省略する他、以下、第2実施形態の特徴部分を中心に説明するものとする。

#### 【0023】

図8、図9は、上述した第1実施形態で示した図5、図6に対応する動作を示したフローチャートである。

まず、書き込み対象のAPソフトを1つ選択すると（ステップC1）、選択指定されたAPソフトを取得し（ステップC2）、また、書き込み対象の端末を指定すると（ステップC3）、その指定内容に応じて指定端末のみの書き込みか、グループ対応書き込みかを調べ（ステップC4）、指定端末のみの書き込みが指定された場合には、指定端末から「製造番号」を読み出す（ステップC5）。そして、それを暗号化するための暗号キーを生成し（ステップC6）、指定端末から読み出した「製造番号」をこの暗号キーで暗号化し、端末識別情報を生成する（ステップC7）。次に、暗号キーを指定端末に書き込むと共に（ステップC8）、指定端末対応のCFカード3にAPソフトを書き込む（ステップC9）。そして、このCFカード3内にそのAPソフトに対応付けてアクセス制御用プログラムを組み込むと共に（ステップC10）、このアクセス制御用プログラム内に暗号化端末識別情報を埋め込む（ステップC11）。これによって指定端末に対する処理が終わると、ステップC12でそのことが検出されてこのフローの終了となる。

#### 【0024】

一方、グループ対応の書き込みが指定された場合には（ステップC4）、図9のフローチャートに進み、まず、上述した第1実施形態と同様に、そのグループ端末識別情報を生成する処理が行われる（ステップC15～C18）。そして、このグループ端末識別情報を暗号化するための暗号キーをランダム生成すると共に（ステップC19）、この生成キーを用いてグループ端末識別情報を暗号化する（ステップC20）。次に、グループ端末識別情報と共に、その暗号化キーを指定端末に書き込む（ステップC21）。そして、図8のステップC9に戻り、

指定端末対応のCFカード3に、APソフト／データを書き込む。そして、このCFカード3内にそのAPソフトに対応付けてアクセス制御用プログラムを組み込むと共に（ステップC10）、このアクセス制御用プログラム内に暗号化端末識別情報を埋め込む（ステップC11）。このような処理は指定グループ内の全端末に対して実行される。すなわち、ステップC12では指定グループ内の全端末終了かを調べ、終了していなければ、ステップC13に進み、同一グループ内の次の端末を指定したのち、図9のステップC15に進み、グループ端末識別情報と共に、その暗号化キーを指定端末に書き込む。以下、指定グループ内の全端末終了まで上述の動作を繰り返す。

#### 【0025】

図10は、上述した第1実施形態で示した図7に対応する動作を示したフローチャートである。

まず、CFカード3がセットされていないければ（ステップD1）、通常処理のメインフローに戻るが、セットされていれば、そのCFカード3内のAPソフト対応のアクセス制御用プログラムを起動させる（ステップD2）。そして、このアクセス制御用プログラムにしたがってCFカード3から端末識別情報を読み出すと共に（ステップD3）、サーバ装置1から自己の端末に書き込まれた端末情報暗号用の暗号キーを読み出し（ステップD4）、この端末識別情報を暗号キーに基づいて複合化する（ステップD5）。そして、予め自己の設定情報である端末識別情報を読み出し（ステップD6）、複合化した端末識別情報と比較し（ステップD7）、両者が一致するかを調べる（ステップD8）。ここで、不一致が検出された場合には、当該カードに対するアクセスを不可として処理終了となるが（ステップD9）、両者の一致が検出された場合には、それに対応するAPソフトを起動可能としてそのアクセスを許可する（ステップD10）。

#### 【0026】

以上のように、この第2実施形態においては、サーバ装置1側で管理しているAPソフト／データを持ち運び自在なCFカード3を介して携帯端末装置2側に外部提供する場合、CFカード3と携帯端末装置2との対応付けを端末識別情報の暗号化、複合化によって行うことで、特定の端末に対してのみAPソフトのアク



セスを許可することができる。この場合、CFカード3内にそのAPソフト毎にアクセス制御用プログラムを組み込むと共に、このアクセス制御用プログラム内に暗号化端末識別情報を埋め込むようにしたから、このアクセス制御用プログラムにしたがってAPソフト毎のアクセス制御が可能となる。

#### 【0027】

なお、上述した各実施形態においては、持ち運び自在な記録媒体としてCFカード3を例示したが、これに限らず、磁氣的、光学的記録媒体等、任意であり、また、クライアント端末はモバイル型の端末に限らず、デスクトップ型の端末であってもよい。また、グループ端末識別情報は、そのグループに属する1台目の携帯端末装置2から読み込んだ固有の製造番号と、任意に入力したグループ名との組み合わせによって生成するようにしたが、1台目の携帯端末装置2から読み込んだ製造番号に限らず、その作成は任意であり、ユニークなグループ端末識別情報であればよい。

#### 【0028】

#### 【発明の効果】

第1の発明によれば、サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部提供する場合、記録媒体と端末装置との対応付けを端末識別情報の一致、不一致およびアプリケーションソフト／データを管理する管理情報の暗号化、複合化によって行うようにしたから、特定の端末装置に対してのみアプリケーションソフト／データのアクセスを許可することができ、セキュリティ維持と共に、アクセス権限を有しない他の装置による不法なコピー複製を効果的に禁止することが可能となる。

第2の発明によれば、サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部提供する場合、記録媒体と端末装置との対応付けを端末識別情報の暗号化、複合化によって行うようにしたから、特定の端末装置に対してのみアプリケーションソフト／データのアクセスを許可することができ、セキュリティ維持と共に、アクセス権限を有しない他の装置による不法なコピー複製を効果的に禁止することが可能となる。特に、記録媒体内において、アプリケーションソフト毎にアクセス制御用プログラム

を組み込むと共に、このアクセス制御用プログラム内に暗号化端末識別情報を埋め込むようにすれば、このアクセス制御用プログラムにしたがってアプリケーションソフト毎のアクセス制御が可能となる。

【図面の簡単な説明】

【図 1】

セキュリティ管理システムの全体構成を示したブロック図。

【図 2】

C F カード 3 の内容を示した図。

【図 3】

端末グループ対応の C F カード 3 を示した図。

【図 4】

サーバ装置 1 / 各端末装置 2 の全体構成を示したブロック図。

【図 5】

サーバ装置 1 側で記憶管理されている A P ソフト / データを持ち運び自在な C F カード 3 を介して端末装置 2 側に外部提供する場合におけるサーバ装置 1 側の動作を示したフローチャート。

【図 6】

図 5 に続くサーバ装置 1 側の動作を示したフローチャート。

【図 7】

C F カード 3 へのアクセスが指定された際に実行開始される各携帯端末装置 2 側での動作を示したフローチャート。

【図 8】

第 2 実施形態において、サーバ装置 1 側で記憶管理されている A P ソフトを持ち運び自在な C F カード 3 を介して端末装置 2 側に外部提供する場合におけるサーバ装置 1 側の動作を示したフローチャート。

【図 9】

図 8 に続くサーバ装置 1 側の動作を示したフローチャート。

【図 1 0】

第 2 実施形態において、C F カード 3 へのアクセスが指定された際に実行開始

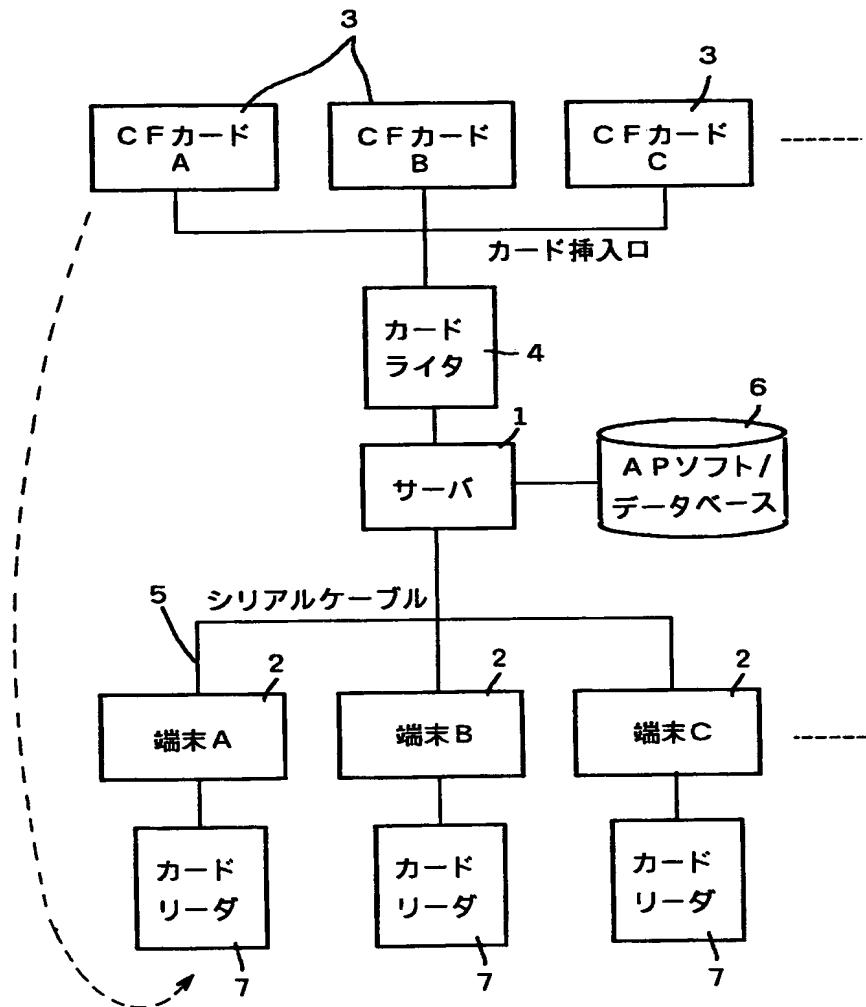
される各携帯端末装置 2 側での動作を示したフローチャート。

【符号の説明】

- 1 サーバ装置 1
- 2 携帯端末装置 2
- 3 C F カード 3
- 4 カードライタ 4
- 6 A P ソフト／データベース格納部 6
- 7 カードライタ 7
- 1 1 C P U
- 1 2 記憶装置
- 1 3 記録媒体
- 1 5 伝送制御部
- 1 6 入力部

【書類名】 図面

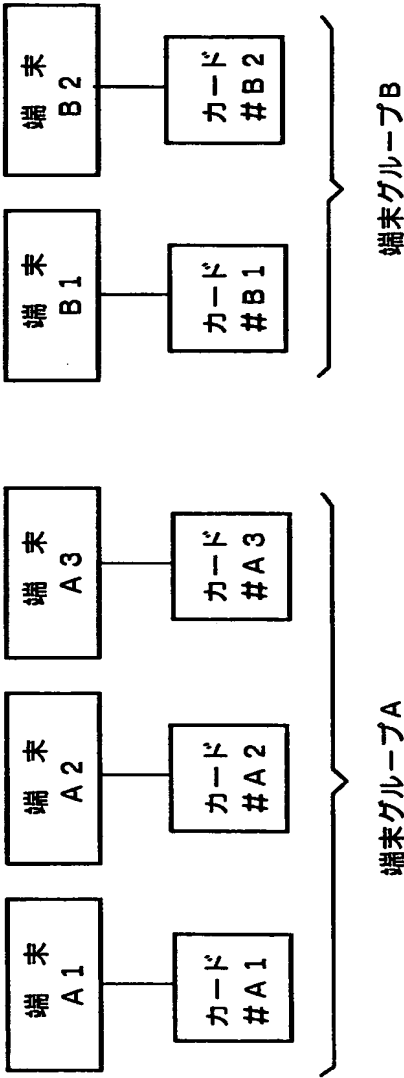
【図 1】



【図 2】

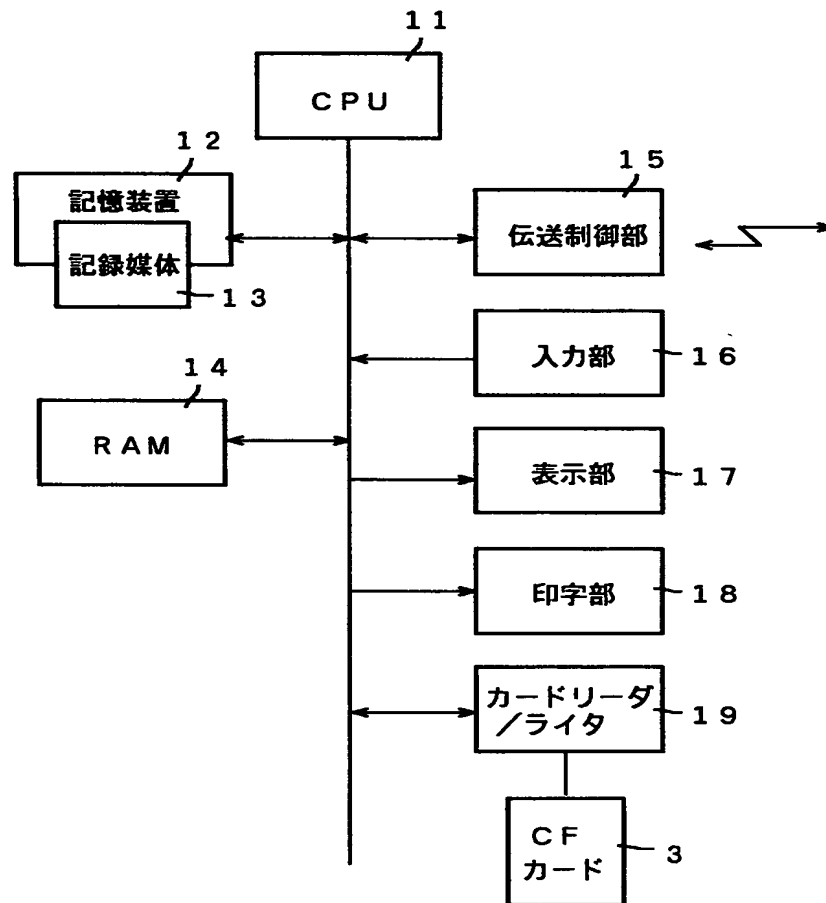
CFカード	
スクランブルフラグ	
暗号化識別番号	
F A T	
ルートディレクトリ	
APソフト／データベース	

【図 3】

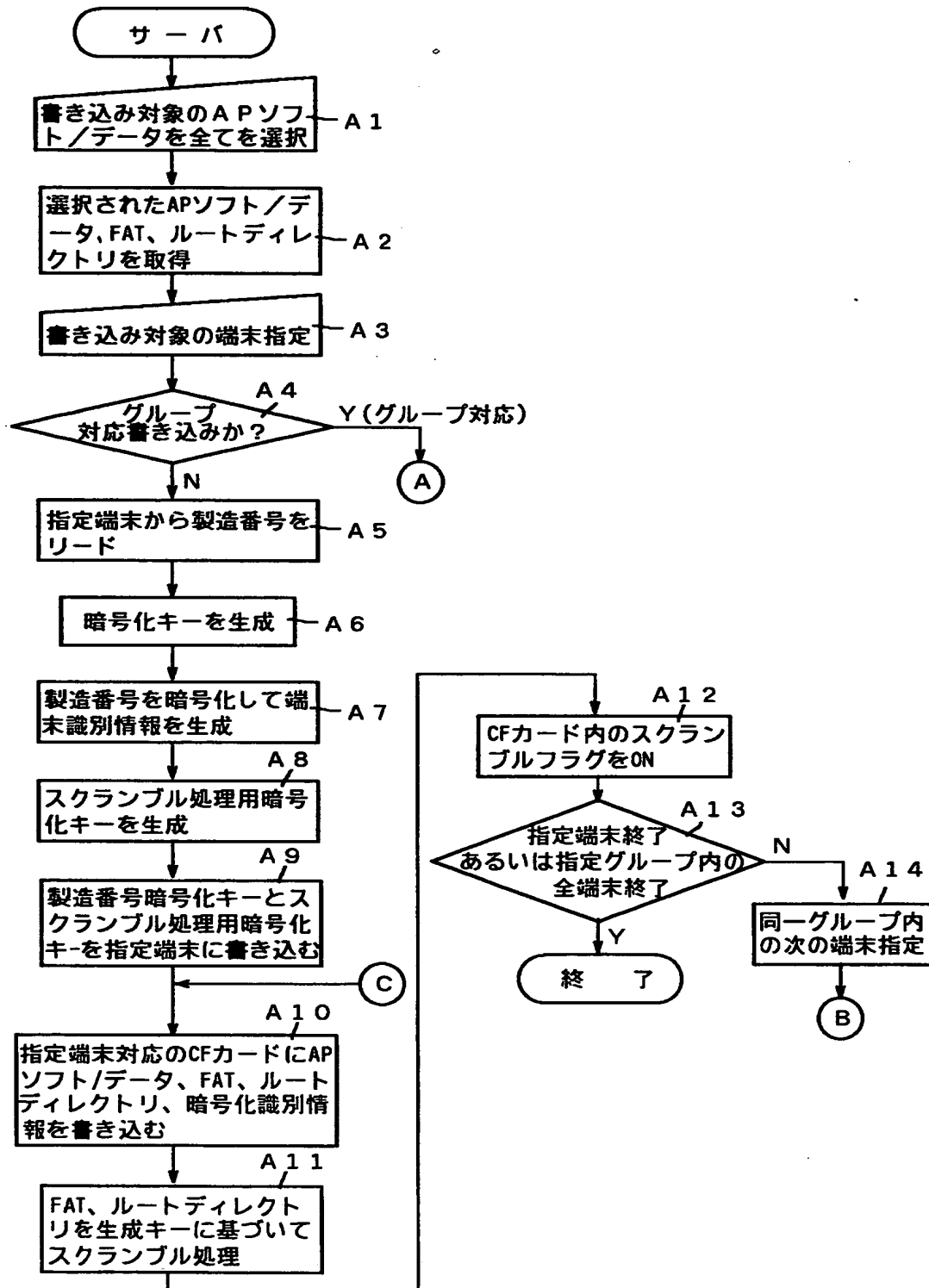


【図 4】

サーバ/端末ブロック図

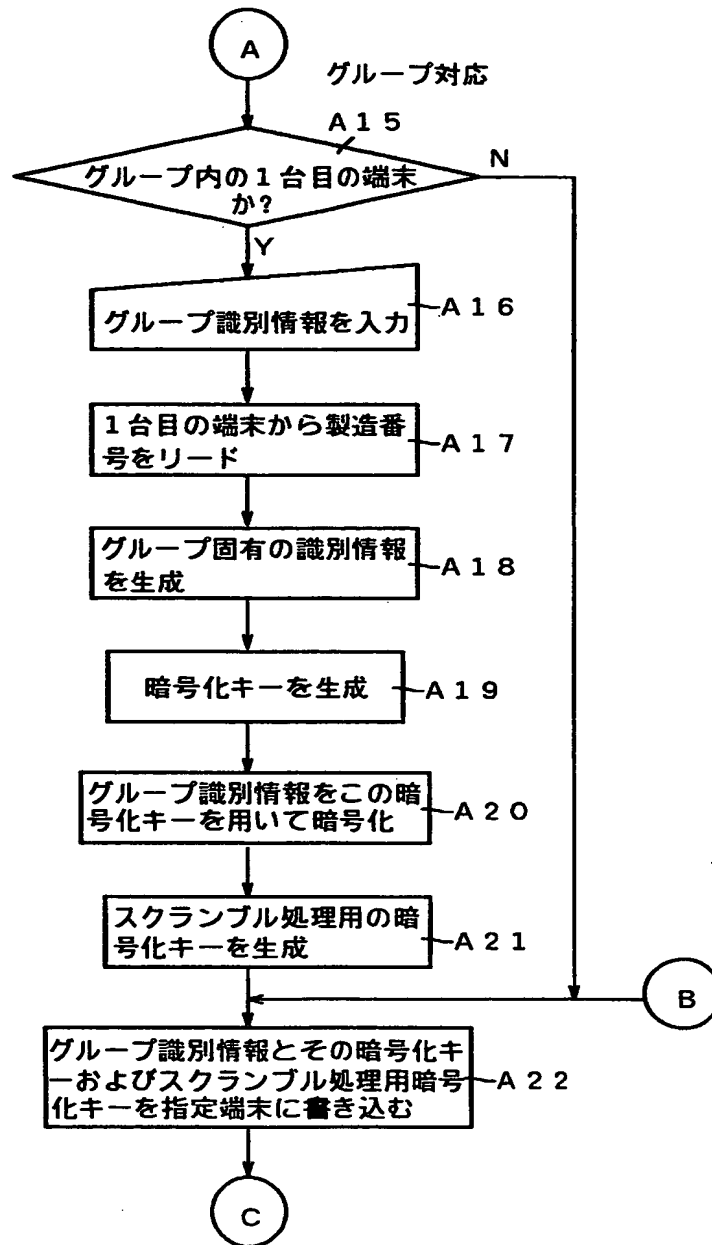


【図 5】

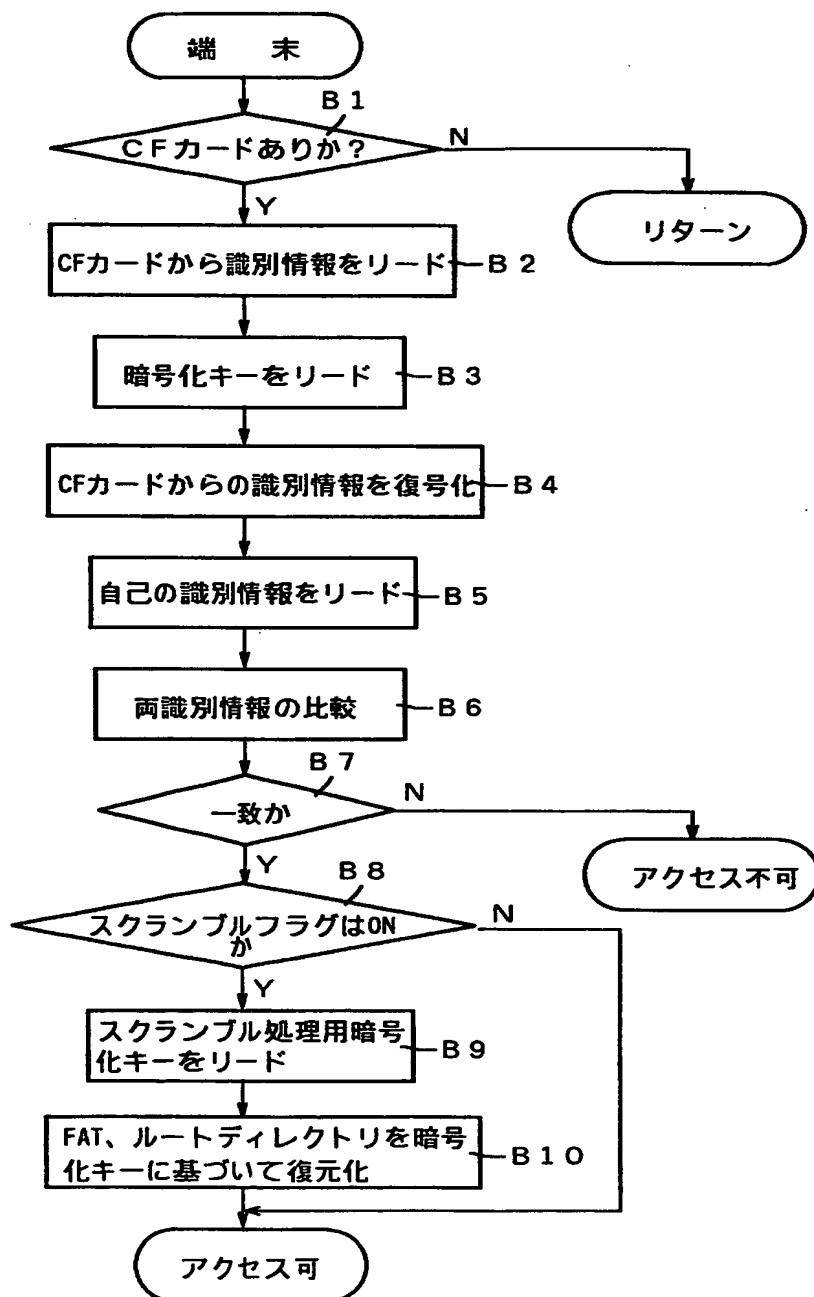




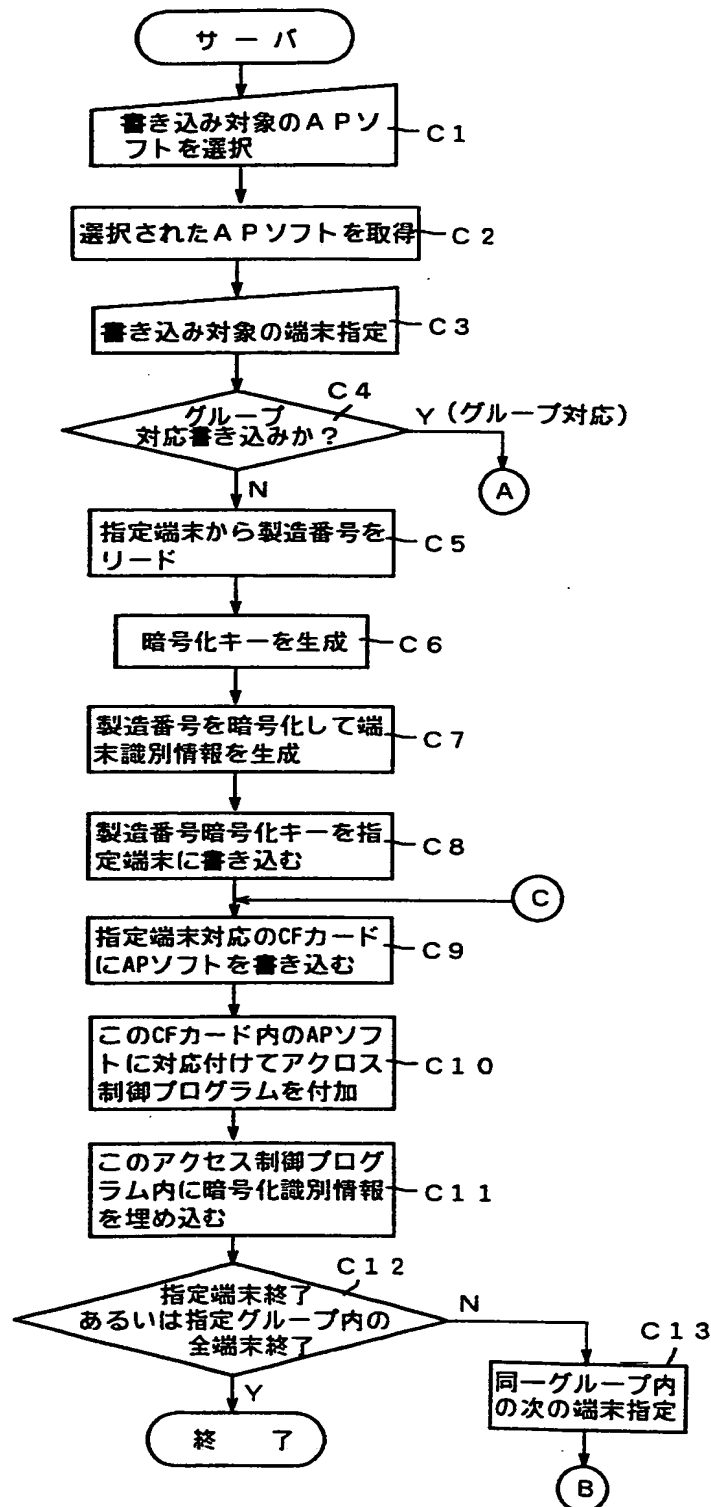
【図 6】



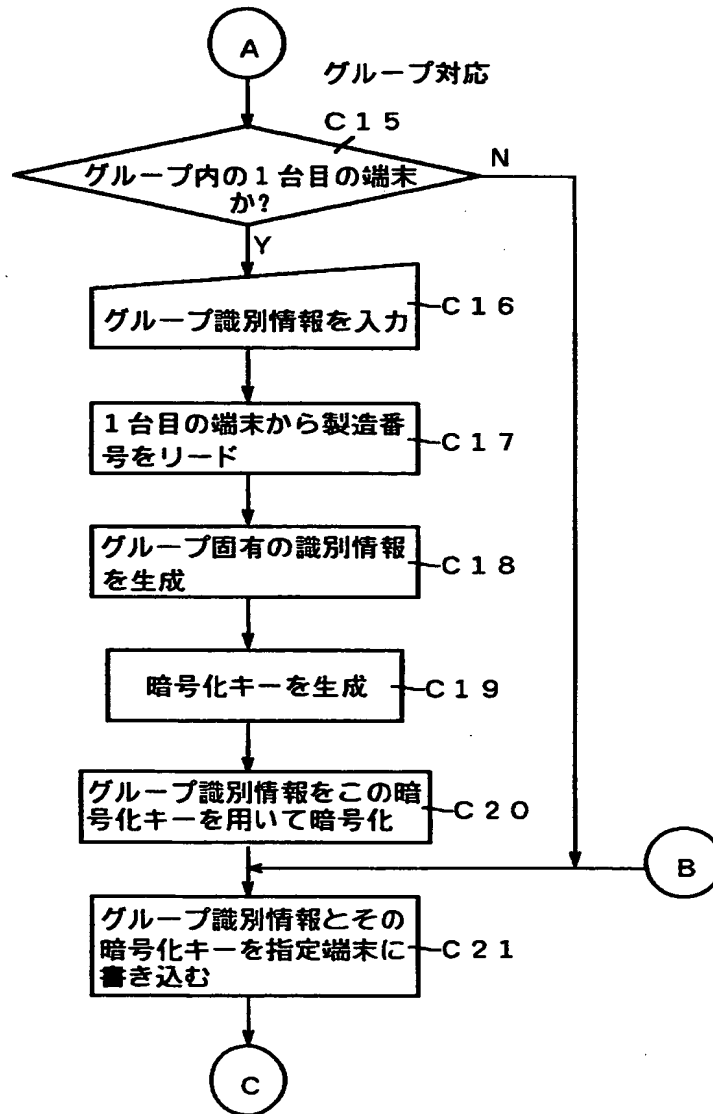
【図 7】



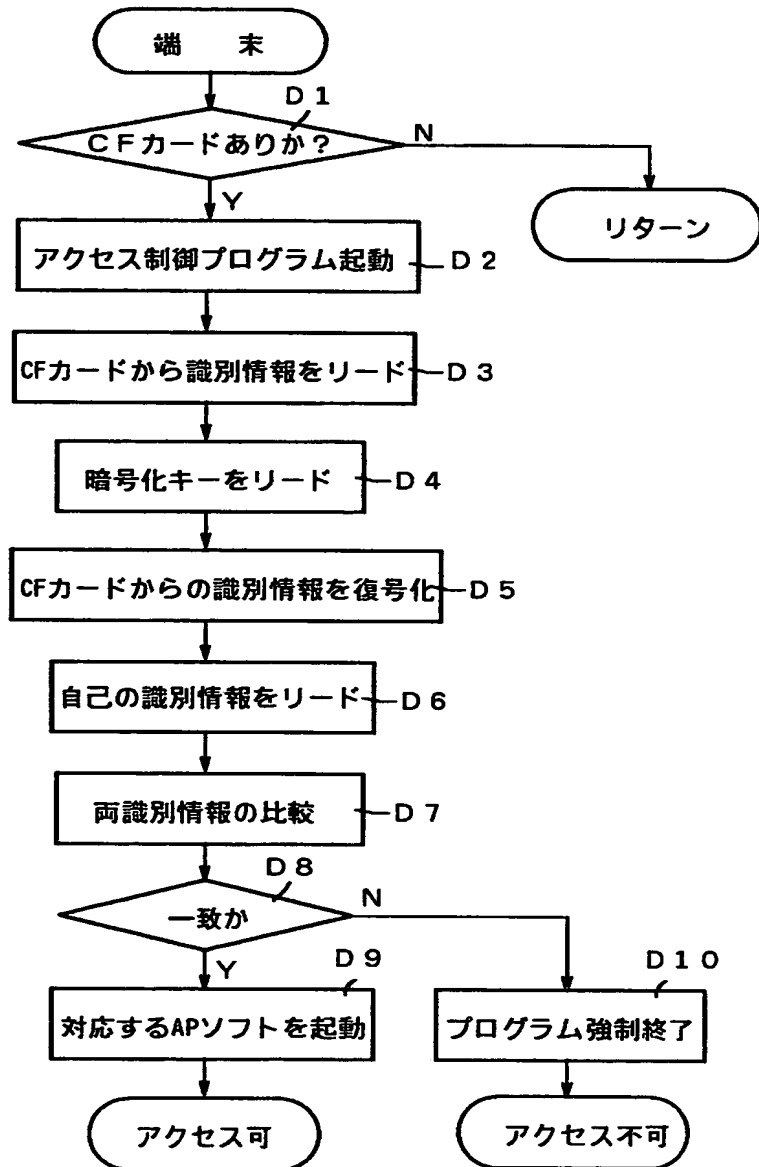
【図 8】



【図 9】



【図 1 0】



【書類名】 要約書

【要約】

【課題】サーバ側のアプリケーションソフト／データをＣＦカードを介して端末側に外部提供する場合、カードと端末との対応付けを端末識別情報の一致、不一致およびアプリケーションソフト／データする管理情報の暗号化、複合化によって行うことで、特定の端末に対してのみ、そのアクセスを許可する。

【解決手段】サーバ１は、端末２から端末識別情報を読み込むと共に、読み込んだ端末識別情報の他、ＡＰソフト／データとそのＦＡＴをＣＦカード３に書き込み、カード３内のＦＡＴをクランブル処理して暗号化する。端末２は、カード３内のＡＰソフト／データをアクセスする際に、当該カード３から暗号化された端末識別情報を読み出してそれを復元し、自己の端末識別情報と比較した結果、それらの一致が検出された際に、スクランブル処理されているＡＰソフト／データのＦＡＴ、ルートディレクトリを復元する。

【選択図】 図１

認定・付加情報

特許出願の番号	平成11年 特許願 第266853号
受付番号	59900916168
書類名	特許願
担当官	第七担当上席 0096
作成日	平成11年10月 7日

<認定情報・付加情報>

【提出日】	平成11年 9月21日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 1 4 4 3 ]

1. 変更年月日	1 9 9 8 年 1 月 9 日
[変更理由]	住所変更
住 所	東京都渋谷区本町 1 丁目 6 番 2 号
氏 名	カシオ計算機株式会社